UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS

EASTERN DIVISION

IN RE: AIMSTER COPYRIGHT LITIGATION	MASTER FILE NO. 01 C 8933 MDL 1425 JUDGE MARVIN E. ASPEN **DECLARATION OF PATRICK BRESLIN IN SUPPORT OF PLAINTIFFS' PROPOSED PRELIMINARY INJUNCTION ORDER**

DECLARATION OF PATRICK BRESLIN

I, Patrick Breslin, the undersigned, declare:

1. I am the Chief Executive Officer of Relatable. I make this declaration in support of Plaintiffs' Proposed Preliminary Injunction Order. I have personal knowledge of the following facts, and if called and sworn as a witness could and would testify competently thereto.

2. Based in Alexandria, Virginia, Relatable is a privately held company founded in November 1999. Relatable is a leading provider of advanced content identification and personalization technologies for the digital delivery of audio and video content. Relatable's patent-pending acoustic fingerprint technology (called TRM) is an industry leader in terms of its

proven ability to accurately identify millions of digital audio files on a mass-market scale and is able to do so without significant negative impact on a large-scale network's performance.

3. In my role as Chief Executive Officer of Relatable, I am responsible for Relatable's overall management as well as business development and finance activities. These include analyzing the business opportunities for our advanced technology solutions, identifying customer prospects for software products such as TRM acoustic fingerprint technology, negotiating software license agreements and managing relationships with customers.

4. Relatable is not affiliated with any of the plaintiffs in this action and does not have a business relationship with any plaintiff.

5. The defendants in this case have stated repeatedly in the news media that there is no way to prevent unauthorized content from being made available over their systems. To the contrary, Relatable has developed a product called TRM, which can be used, among many other uses, to identify digital audio files that a user places in his or her "share folder" on a peer-to-peer ("P2P") file-trading system, such as the P2P systems operated in this litigation. TRM allows a licensee to identify unauthorized files that a user places in his or her "share folder" so that it can block them from being available to other users in the system. TRM can be implemented in a P2P system, as described below.

6. TRM software is a client-server solution. A layer of TRM software is integrated into a client application, such as a P2P application on the user's PC, through which TRM generates identifiers for song files users place in their "share folders." The TRM client layer sends the identifiers (called "acoustic fingerprints" and described further below) to a TRM server within the P2P network's infrastructure. The TRM server contains a reference database of fingerprints and determines whether the fingerprint generated on the client PC matches the

fingerprint of an existing recording in the database, to determine whether access to the user's file should be allowed.

7. The largest scale usage of TRM was when Napster integrated the technology into its P2P network, to allow the robust identification of audio content that users designated for file sharing. These fingerprints were in turn used to allow the filtering (using a "filter in" model as described below) of users' files, to prevent further file-sharing of copyrighted works not under license. TRM has also been used to identify radio station broadcasts, by generating radio airplay logs in the US and Europe, and for CD content identification.

RELATABLE'S TRM TECHNOLOGY

8. TRM is a technology that generates a unique "acoustic fingerprint" for a digital audio file that is based entirely on the acoustical properties of the recording the file represents. Much like a human fingerprint, an acoustic fingerprint identifies with virtual certainty the recording's unique acoustical properties.

9. The TRM software generates this acoustic fingerprint by analyzing a large number of the acoustic properties of the sound contained in the digital audio file. TRM breaks down a recording into segments and then takes measurements of certain acoustic properties of each segment. Using a special algorithm, the resulting measurements are transformed into a code, which is unique to each recording. (An algorithm is simply a detailed sequence of actions that the software instructs the computer to perform to accomplish a specific task – here, the creation of the fingerprint.) Using this method, TRM generates a unique code (the fingerprint) for each recording, as well as for each digitized copy of any given recording of a song, with different codes for live tracks, remixes, and performances of the same work by different artists. Just as a person's fingerprint is much smaller than the entire person but still positively identifies the person, the fingerprint that TRM generates is much smaller than the recording itself, because the

fingerprint extracts only certain unique identifying information about the sonic properties of the recording. For example, an acoustic fingerprint for one song recording would be about 1500 bytes of data, compared to about 3 megabytes of data (2,000 times the size of the fingerprint) for the recording itself in a compressed format, such as MP3, and 50 megabytes of data (over 30,000 times the size of the fingerprint) for a song in an uncompressed digital format. This much smaller size makes the fingerprint easy to store, send, and compare to fingerprints for other recordings.

10. Audio files can be digitally encoded in a variety of formats, each of which uses a particular algorithm to compress the data to reduce the amount of space the file uses on the computer, making it easier for the user to both store and transfer the file. Some formats, including MP3, reduce the size of the file by discarding unnecessary data, such as sound frequencies that are outside the range of human hearing. TRM can identify audio files that have been encoded using any of the most popular digital audio formats, including MP3, Ogg Vorbis, Real, or Windows Media Audio.

11. TRM also identifies digital audio files at widely varying bit rates. The bit rate is the number of bits (small pieces of data) that pass a given point in a network in a given amount of time, usually a second. Thus, a bit rate is usually measured in some multiple of bits per second - for example, kilobits, or thousands of bits per second (Kbps). The higher the bit rate, the larger the file and the better the sound quality. Users can set the bit rate at several different levels, but TRM will accurately identify audio at bit rates from the highest quality down to 16 Kbps or below, bit rates that are far below AM quality, for example. Users generally prefer audio files compressed at much higher quality bit rates, at least 56Kbps and more often 96Kbps, 128Kbps or above.

12. Because it interprets the kind of audio information that humans actually hear, TRM can be used to identify an audio file regardless of whether the person providing the file has accurately labeled the recording, or has labeled it at all. For example, TRM recognizes the

recording, whether or not the song title, artist name, or other related information is accurate or available.

13. Integral to the TRM system is a reference fingerprint database, which consists primarily of fingerprints of digital audio files provided by companies that license TRM (for example, a record company that owns the copyrights to recordings), or obtained from a third party that has such databases, such as Loudeye, Muze, and Reciprocal. TRM creates a digital fingerprint of each recording supplied by the licensee or third party in the manner described above, and stores that fingerprint in the reference database.

14. The reference database also includes "metadata" associated with each audio file. Metadata is literally "data about data" – including textual information like artist, title, album, and label, and electronic data, such as track duration. Metadata can be mapped to the fingerprint in a database without affecting the quality of the sound. Thus, the reference database includes both an audio fingerprint of each recording and associated metadata that identifies the recording that has been fingerprinted.

15. TRM identifies an unknown digital recording by generating a fingerprint of the unknown recording (in the same way it generated the fingerprints in the reference database), and comparing that fingerprint at a very high speed to the fingerprints in the reference database. (In internal tests, a commercial version of TRM was able to handle over 5000 fingerprint matches per second, or up to billions of queries per day. Actual match rates vary depending on the size of the fingerprint database. However, under real world conditions with many millions of fingerprints in a database, TRM has been proven to handle query rates in the thousands per second per server. Adding servers to the system proportionately increases the number of queries the system can handle by an equal factor.) If the fingerprint of the unknown recording matches a fingerprint in the reference database, TRM identifies the unknown recording as a copy of the matching recording in the reference database. Using the metadata stored in the reference database

along with the digital fingerprints, TRM identifies the unknown recording by artist, title, album, label, etc., depending on the availability and accuracy of such metadata in the database.

16. If the fingerprint of the unknown recording does not match any fingerprint of a known recording in the reference database, TRM can, if desired, add the newly created fingerprint of the unknown recording to the reference database, together with any metadata associated with that specific file.

IMPLEMENTATION IN A P2P SYSTEM

17. I am familiar with P2P systems generally, including the defendants' P2P systems through news articles and other publicly available information. I am generally familiar with the architecture of the systems and their mode of operation.

18. TRM software solutions are available to license, including to defendants.

19. TRM can operate in two different ways to enable recordings to be blocked from being made available without authorization from the copyright holder on defendants' P2P systems. First, TRM can create a reference database of fingerprints of recordings that are authorized for distribution. Then, when TRM compares the fingerprints of recordings that P2P users make available to all of the fingerprints in that reference database, if the fingerprint of an available recording matches a fingerprint in the reference database, the P2P system will permit the recording to be available to other users, but, if there is no match, the P2P system will block the recording from being made available. This is commonly known as a "filter-in" mechanism. This is essentially a highly automated way for each user of the P2P system to seek permission from the rights holders before making a copyrighted recording available.

20. Alternatively, TRM can create a reference database of fingerprints of protected recordings, i.e., recordings that are not authorized to be made available to other users in the P2P system. In this scenario, when TRM compares the fingerprints of recordings that P2P users make available to all of the fingerprints in that reference database, if the fingerprint of the offered recording matches a fingerprint in the reference database, the P2P system will block the offered recording from being available to other users, but if there is no match, will permit the offered recording to be available to other users. This is commonly known as a "filter-out" mechanism. In a modified form, a "filter-out" system would track the unmatched recordings that are available, via the acoustic fingerprint, to allow for future compensation of copyright holders for all distribution of the digital recording.

21. TRM could be used in a P2P system without any significant degradation in the system in different ways depending on the architecture of the system itself. The TRM servers are designed to function in a scalable cluster, where the system can increase the number of queries per second it can handle by simply adding additional servers to the cluster. This allows a central cluster of only a dozen servers to handle tens of thousands of queries per second, which reduces to a minimum any potential network degradation for introducing content identification in a central fashion to a P2P network. Additionally, it is possible to develop a distributed version of TRM, for decentralized P2P networks, which would allow the distribution of the content identification database and resolution tasks throughout the P2P network. In both cases, due to the inherent scalability and speed of TRM, integration with a network performing even billions of transactions per day is feasible.

22. Because of the broad range of acoustic properties that TRM uses to create the fingerprint, I believe that any effort to alter an audio recording to circumvent TRM would have to be so significant that it would audibly degrade the quality of the audio file.

Received 09/09/2002 05:21PM in 04:40 from 703 212 4900 on line [5] * Pg 9/9
SEP-10-2002 08:18 AM RELATBLE 703 212 4900 P.09

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on September 9, 2002, at Alexandria, Virginia.

PATRICK BRESLIN